IN THE UNITED STATES DISTRICT COURT FOR MARYLAND,
SOUTHERN DISTRICT

BEYOND SYSTEMS, INC.,	)	
Plaintiff,	)	
v.	)	Case No. PJM 08 cv 0921
WORLD AVENUE USA, LLC, *et al.*,	)	
Defendants.	)	

AFFIDAVIT OF PAUL A. WAGNER REGARDING

CONFIDENTIALITY OF THE EMAILS AT ISSUE

I, Paul A. Wagner, state that:

1. I am over 18 years of age and fully competent to testify to the facts set forth in this Declaration.

2. Beyond Systems, Inc. ["BSI"] provides Internet services involving domain names it owns or that its customers own.

3. BSI actively monitors some email addresses, such as the email addresses it uses (including those at issue in this suit). BSI delivers emails addressed to other email addresses privately to external clients without manual inspection by BSI.

4. Based on my knowledge in the industry, most ISPs who sue spammers (including Microsoft, AOL, Verizon, Yahoo and Earthlink) do so primarily on the basis of spam sent to spamtrap and fallow (a.k.a. reclaimed) email addresses, not the email addresses of their current users. BSI does the same in part. Most ISPs do not involve their customers in their litigation; BSI likewise seeks to avoid exposing its customers to defendants like World Avenue and the

spammers they hire. One exception to this noninvolvement was when AOL returned to its customers the "ill-gotten bounty" seized from spammers: see http://www.theregister.co.uk/2005/08/10/aol_spam_sweepstake/ .

5. I have observed that the major ISPs generally keep their email addresses confidential in litigation, for several reasons, and I am familiar with the following examples. Paragraphs 6 and 7 of Exhibit C1, which is the Declaration of David Vetter, Program Manager for Microsoft's MSN Hotmail web-based email service, indicate that Microsoft's confidential "trap" accounts were used in spam litigation. Both Microsoft and the FTC keep recipient email addresses confidential. The FTC refuses to turn over the recipient addresses under FOIA requests, charging $1 per email to redact all such personal identifying information. The FTC keeps emails at issue confidential in its prosecutions by the Justice Department.

6. Kraft Foods, Connexus Corporation, Hydra Media and World Avenue all use a vendor named LashBack to inform them about abuse from their affiliates. [See http://www.lashback.com/about/FeaturedClients.aspx] LashBack actively seeds and maintains secret email addresses for the core purpose of receiving spam. In particular, LashBack opts out unique email addresses in spam it has already received, and then observes whether that unique opt-out gets a hit. In the BSI v. Kraft litigation, LashBack sought to keep its discovery responses confidential, particularly its opted-out email addresses. [See LashBack's letter in Exhibit C2.] According to that letter, LashBack seeks to protect its email addresses for reasons of privacy (e.g., so they won't receive spam or other abuses) and because the confidentiality of the addresses has business value to LashBack.

7. I have observed that spammers stop spamming to email addresses they learn are received by people who investigate spam, submit reports of spam to advertisers or law

enforcement, and/or litigate spam, but continue or commence spamming to other email addresses, and I cite the following examples based on my person knowledge:

- the bulk emailer to whom I attribute most of the emails at issue, Sebastian Barale, stopped receiving "Gevalia" emails in March 2005 after one of BSI's Internet service providers, Hypertouch, Inc., had complained to Kraft about the spam multiple times in the prior four months; however, Mr. Barale continued spamming on behalf of World Avenue (and Connexus Corporation) until September 2005;
- the AccelBiz spammer has halted spamming to certain emails addresses that were produced to the Defendants, but continued spamvertising Hydra products to other BSI email addresses;
- MBP Advertising, who was a defendant in BSI v. Keynetics, blacklisted domain names of BSI, Microsoft, Yahoo, Earthlink, but not Gmail (who to my knowledge has never sued a spammer); the confidentiality of specific email addresses forced MBP to blacklist entire domains;
- after Joe Wagner won a damage judgment against World Ave in a small claims suit in California, Joe ceased to receive spam from World Avenue's spammer to his Stanford University address; however, World Avenue continues to use this same spammer, two years later and despite BSI's suit.

8. Prior discovery in BSI v. Kraft has shown that Kraft, Connexus and Hydra place the email addresses from recipients who complain onto so-called opt-out or suppression lists, and then make those lists available to their affiliates or subaffiliates -- i.e., to hundreds or thousands of spammers. Similarly, while BSI is still waiting for discovery responses from World Avenue, indications that World Avenue disseminates email addresses to affiliates include

http://livenudefrogs.com/abuse/emarketresearchgroup.com/ . The Defendants send these email addresses unencrypted, rather than sending only the hash of each email address.World Avenue hired the top 2 "worst" spammers, according to Spamhaus.org [Exhibhit C3]. Microsoft and the New York State attorney general Eliot Spitzer filed joint lawsuits in 2003 against Scott Richter/OptinRealBig, World Ave hired Richter/OptinRealBig to send spam in April 2005, based on the redirections of sales URLs in 593 emails at issue. (These 593 are distinct from the 595 Ralsky spam at issue in BSI v. Kraft, likewise sent in April 2005.) Richter turned around and outsourced to convicted spam felon Alan Ralsky. [Exhibit 3 to original Complaint] Exhibits C4 and C5 show sample emails at issue where BSI's email addresses appear in multiple places (underscored), often encoded, throughout the email. There might be additional encoded identifiers that I don't yet understand but that third parties do.

9. In summary, the basic reasons why BSI wants to protect its email addresses is that (1) the ad networks in these actions, such as World Avenue, have a long history of passing on email addresses to their spammers, contrary to industry best practice, (2) defendants acknowledge the value and purpose of keeps said email addresses confidential when they hire Lashback, (3) to avoid getting more spam or abuse to the disclosed address which include active contact email addresses required for clients, (4) to avoid nullifying the disclosed addresses and ramping up spam to the non-disclosed addresses, and (5) for the above reasons BSI regards the emails to be confidential research, development, or commercial information.

I provide the following declaration I declare under penalty of perjury that the foregoing is true and correct.

Date: November 2, 2009

By: